UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/981,182	10/16/2001	John M. Schnizlein	50325-0560	5410

29989 7590 05/16/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/981,182	SCHNIZLEIN ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 3/4/02
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending in the application.

2. Claims 1-27 have been rejected.

Specification

3. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract exceeds the 150-word limit.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-3, 6, 7 and 9-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Demirtjis et al U.S. Patent No. 6,697,864 B1.

As to claim 1, Demirtjis et al discloses a method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, at the intermediate device from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information [column 5, lines 39-52];

receiving, at the intermediate device from the host, a first message for discovering a logical network address for the host [column 7, lines 19-30];

generating a second message based on the first message and the first data [column 7, lines 19-30]; and

sending the second message to a second server that provides the logical network address for the host [column 7, lines 19-30].

As to claim 2, Demirtjis et al discloses a method as recited, wherein:

an authenticator process performs the step of receiving the first data [column 8, lines 35-67];

a relay agent process for the second server performs the steps of receiving the first message and sending the second message [column 8, lines 35-67];

the relay agent process is separate from the authenticator process [column 8, lines 35-67]; and

the step of generating the second message further comprises the step of sending a third message, from the authenticator process to the relay agent process, based on the first data [column 8, lines 35-67].

As to claim 3, Demirtjis et al discloses a method as recited, wherein:

an authenticator process performs the step of receiving the first data [column 8, lines 35-67];

a relay agent process for the second server performs the steps of receiving the first message and sending the second message [column 8, lines 35-67];

the relay agent process is separate from the authenticator process [column 8, lines 35-67]; and

the step of generating the second message further comprises the steps of:

storing second data based on the first data by the authenticator process [column 8, lines 35-67]; and

retrieving the second data by the relay agent process in response to the step of receiving the first message [column 8, lines 35-67].

As to claim 6, Demirtjis et al discloses that the physical connection comprises an Ethernet interface card on the intermediated device [column 5, lines 6-38].

As to claim 7, Demirtjis et al discloses that the physical connection comprises a wireless Ethernet encryption key and time slot [column 5, lines 6-38].

As to claim 9, Demirtjis et al discloses that the second message is based on a dynamic host configuration protocol (DHCP) [column 5, lines 6-38].

As to claim 10, Demirtjis et al discloses that the first data includes user class data indicating a particular group of one or more authorized users of the host [column 9, lines 1-24]. Demirtjis et al discloses that the step of generating the second message is further based on the user class data [column 9, lines 1-24].

As to claim 11, Demirtjis et al discloses a method as recited, wherein:

the first data includes credential data indicating authentication is performed by the first server [column 9, lines 1-24], and

the step of generating the second message is further based on the credential data [column 9, lines 1-24].

5. Claims 12 and 13 are rejected under 35 U.S.C. 102(b) as being anticipated by Hobbs U.S. Patent No. 5,987,454.

As to claim 12, Hobbs discloses a method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, from the host, a first request for access to a network connected to the intermediate device, the first request including information about a user of the host [column 10 line 6 to column 11 line 19];

sending a second request for authentication of the physical connection to a first server that provides authentication and authorization, the second request based on the first request [column 10 line 6 to column 11 line 19];

receiving, at the intermediate device from the first server in response to the second request, first data indicating at least some of authentication and authorization information [column 10 line 6 to column 11 line 19];

enabling the physical connection to forward subsequent messages between the host and a network connected to the intermediate device [column 10 line 6 to column 11 line 19]; and

storing the first data at least until a message is received from the host for discovering a logical network address for the host [column 10 line 6 to column 11 line 19].

As to claim 13, Hobbs discloses a method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, at the intermediate device from the host, a message for discovering a logical network address for the host [column 14 line 46 to column 15 line 28];

retrieving, from a persistent store at the intermediate device, first data indicating at least some of authentication and authorization information received from a first server that provides authentication and authorization in response to a request for authentication of the physical connection [column 14 line 46 to column 15 line 28];

generating a second message based on the first message and the first data [column 14 line 46 to column 15 line 28]; and

sending the second message to a second server that provides the logical network address for the host [column 14 line 46 to column 15 line 28].

6. Claims 14-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Fijolek et al U.S. Patent No. 6,553,568 B1.

As to claim 14, Fijolek et al discloses a method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, from the intermediate device, a first message for discovering a logical network address for the host, the first message including first data indicating at least some of authentication and authorization information from a first server that provides authentication and authorization in response to a request for authentication for the physical connection [column11 line 30 to column 12 line 28];

selecting a particular pool of one or more logical network addresses, from among a plurality of pools of one or more logical network addresses, based on the first data [column11 line 30 to column 12 line 28]; and

sending to the host a second message including second data indicating a particular network address from the particular pool [column11 line 30 to column 12 line 28].

As to claim 15, Fijolek et al discloses that each pool of the plurality of pools is associated with a corresponding group of a plurality of groups of one or more authorized users of the host [column 14, lines 20-32].

As to claim l6,Fijolek et al discloses that the first data includes user class data indicating a particular group of the plurality of groups [column 14, lines 20-32].

As to claim 17, Fijolek et al discloses that the particular pool is associated with a privilege to access an Internet through a gateway process [column 9, lines 42-58].

As to claim 18, Fijolek et al discloses a method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, from the intermediate device, a first message for discovering a logical network address for the host [column11 line 30 to column 12 line 28],

receiving first data from a first server that provides authentication and authorization in response to a request for authentication for the physical connection, the first data indicating at least some of authentication and authorization information [column11 line 30 to column 12 line 28];

selecting a particular pool of one or more logical network addresses, from among a plurality of pools of one or more logical network addresses, based on the first data [column11 line 30 to column 12 line 28]; and

sending to the host a second message including second data indicating a particular network address from the particular pool [column11 line 30 to column 12 line 28].

As to claim 19, Fijolek et al discloses the step of correlating the first message and the first data [column 14 line 54 to column 15 line 40].

As to claim 20, Fijolek et al discloses a method, wherein:

the first message includes a unique identification for the host [column 14 line 54 to column 15 line 40];

the first data includes the unique identification for the host [column 14 line 54 to column 15 line 40]; and

the step of correlating the first message and the first data is based on the unique identification for the host [column 14 line 54 to column 15 line 40].

As to claim 21, Fijolek et al discloses that the unique identification for the host is a media access control address [column 14 line 54 to column 15 line 40].

7. Claims 22 and 24-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Schutte et al U.S. Patent No. 6,405,253 B1.

As to claim 22, Schutte et al discloses a method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, from the intermediate device at an authorization server on a network connected to the intermediate device, a request for authenticating the host, the request including information provided from the host [column 18, lines 7-32];

determining whether the host is authentic and authorized to connect to the network based on user profile data in persistent store and the request [column 18, lines 7-32];

sending, to the intermediate device, a response indicating whether the host is authentic and authorized [column 18 line 44 to column 19 line 50]; and

if it is determined that the host is authentic and authorized, then sending first data based on the user profile data to a configuration server that provides a logical network address for the host [column 18 line 44 to column 19 line 50].

As to claim 24, Schutte et al discloses a computer-readable medium carrying one or more sequences of instructions for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving, from the host, a first request for access to a network connected to the intermediate device, the first request including information about a user of the host [column 18, lines 7-32];

sending a second request for authentication of the physical connection to a first server that provides authentication and authorization, the second request based on the first request [column 18, lines 7-32];

receiving, at the intermediate device from the first server in response to the second request, first data indicating at least some of authentication and authorization information [column 18 line 44 to column 19 line 50];

enabling the physical connection to forward subsequent messages between the host and the network [column 18 line 44 to column 19 line 50]; and

storing the first data at least until a message is received from the host for discovering a logical network address for the host [column 18 line 44 to column 19 line 50].

As to claim 25, Schutte et al discloses a computer-readable medium carrying one or more sequences of instructions for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving, at the intermediate device from the host, a message for discovering a logical network address for the host [column 18, lines 7-32];

retrieving, from a persistent store at the intermediate device, first data indicating at least some of authentication and authorization information received from a first server that provides authentication and authorization in response to a request for authentication of the physical connection [column 18, lines 7-32];

generating a second message based on the first message and the first data; and

sending the second message to a second server that provides the logical network address for the host.

As to claim 26, Schutte et al discloses an apparatus for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, comprising:

means for receiving, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information [column 18, lines 7-32];

means for receiving, from the host, a first message for discovering a logical network address for the host [column 18 line 44 to column 19 line 50];

means for generating a second message based on the first message and the first data [column 18 line 44 to column 19 line 50]; and

means for sending the second message to a second server that provides the logical network address for the host [column 18 line 44 to column 19 line 50].

As to claim 27, Schutte et al discloses an apparatus for assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom [column 18, lines 7-32];

a physical connection that is coupled to the host [column 18, lines 7-32];

a processor [column 18, lines 7-32];

one or more stored sequences of instructions which, when executed by the processor [column 18, lines 7-32], cause the processor to cant' out the steps of:

receiving, through the network interface from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information [column 18, lines 7-32];

receiving, through the physical connection from the host, a first message for discovering a logical network address for the host [column 18 line 44 to column 19 line 50];

generating a second message based on the first message and the first data [column 18 line 44 to column 19 line 50]; and

sending through the network interface the second message to a second server that provides the logical network address for the host [column 18 line 44 to column 19 line 50].

8. Claim 23 is rejected under 35 U.S.C. 102(e) as being anticipated by Baize U.S. Patent No. 6,317,838 B1.

As to claim 23, Baize discloses a method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:

receiving, from the intermediate device at an authorization server on a network connected to the intermediate device, a request for authenticating the host, the request including information provided from the host for a particular user of the host [column 5, lines 34-65];

determining whether the particular user is authentic and authorized to connect to the network based on user-profile data in persistent store and the information provided from the host [column 5, lines 34-65]; and

if it is determined that the particular user is authentic and authorized, then sending, to the intermediate device, a response indicating the host is authentic and authorized [column 6 line 33 to column 7 line 31], wherein:

the response includes data indicating a particular group of one or more users authorized for a particular set of network operations [column 6 line 33 to column 7 line 31],

each network operation in the particular set is controlled by a logical network address of a host of a user [column 6 line 33 to column 7 line 31], and

the group includes the particular user [column 6 line 33 to column 7 line 31].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Demirtjis et al U.S. Patent No. 6,697,864 B1 as applied to claim 1 above, and further in view of Lloyd et al U.S. Patent No. 6,219,790 B1.

As to claims 4 and 5, Demirtjis et al does not teach that the first server is an authentication, authorization and accounting server. Demirtjis et al does not teach that the first server is a RADIUS protocol server.

Lloyd et al teaches a server that is an authentication, authorization and accounting server [column 5 line 65 to column 6 line 5]. Lloyd et al teaches a server that is a RADIUS protocol server [column 5 line 65 to column 6 line 5].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Demirtjis et al so that the first server would have been a authentication, authorization and accounting server (AAA server). The AAA server would have employed a RADIUS protocol.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Demirtjis et al by the teaching of Lloyd et al because by having a AAA server that employs a RADIUS protocol it makes a network capable of supporting a variety of authentication transport protocols from a variety of client types [column 2, lines 48-57].

10. Claim 8 rejected under 35 U.S.C. 103(a) as being unpatentable over Demirtjis et al U.S. Patent No. 6,697,864 B1 as applied to claim 1 above, and further in view of Bahl et al U.S. Patent No. 6,782,422 B1.

As to claim 8, Demirtjis et al does not teach that the request for authentication is based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard.

Bahl et al teaches authentication based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard [column 11, lines 52-58].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Demirtjis et al so that the request for

authentication was based on an Institute of Electrical and Electronics Engineers (IEEE) 802.1x standard.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Demirtjis et al by the teaching of Bahl et al because that standard of protocol is more secure connection and higher level of authentication [column 11, lines 52-58].

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
May 9, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100